GUARDKNOX

GUARDKNOX EV ECU PLATFORM

HIGHLIGHTS

- Comprehensive & robust hardware and software-based solution for secure V2G communication
- High-performance, flexible and scalable platform for the EV industry
- Coupled with patented Secure Service Oriented Architecture (SOA) stack for access control and service level partitioning to secure further levels of connectivity & customization
- Patented Communication Lockdown™ methodology for multi-layer cyber protection
- Foundational layer for added levels of connectivity, services, personalization and new revenue streams for OEMs
- Unique hardware approach

A HIGH-PERFORMANCE EV PLATFORM: THE FOUNDATION FOR CONNECTIVITY AND CUSTOMIZATION

As vehicle complexity and connectivity requirements increase, the need for post-production scalability and extensibility is rising. Furthermore, a secured end-point within the vehicle becomes increasingly vital to the automotive value chain.

GuardKnox's Secure EV ECU offers vehicle cybersecurity protection from cyber threats emanating from the connectivity to the grid and/or a compromised electric charging station (EVSE). The EV ECU is completely autonomous and eliminates the need for human intervention in the security mitigation process. It has high-performance data processing capabilities, does not require external connectivity, constant communication, cloud connectivity, or any on-going updates.

GUARDKNOX EV ECU

Suitable for AC & DC charging, the EV ECU provides a secure endpoint for high-performance data processing and storage while also supporting secure cloud communication, data analytics and AI. The patented software core and hardware architecture enables compliance with not only safety and security standards, but also EV specific protocols - ISO 15118 and DIN SPEC.

The GuardKnox EV ECU for electric vehicles is uniquely suitable for protecting EVs from the cyber threats posed by vehicle-to-grid (V2G) communications by:

- Examining all Vehicle-to-Grid communication to and between the EV and the charging station (EVSE)
- Managing and monitoring the grid charging procedure
- Maintaining and ensuring the safety of charging operation
- Enforcing and ensuring the security of sensitive data and the in-vehicle network from all current and future external threats.

With a full software stack and hardware architecture, GuardKnox's patented technologies adheres to security (ISO 15408), safety (ISO 26262) standards and upcoming ISO 21434. The EV ECU complies with GDPR (General Data Protection Regulation) and provides automotive cybersecurity that easily fits the automotive tiered value chain.

FREEDOM TO EVOLVE

Component	Description
SoC	Cortex-A9 32-bit microprocessor FPGA OR Cortex-M4 32-bit microcontroller
Memory (RAM)	Up to 2GB
Storage (Flash)	Up to 16 GB
Interfaces	HomPlug GreenPHY PLC WiFi CAN 2.0B PWM DIO CAN-FD Ethernet
Symmetric Encryption	AES128, AES256 with GCM, CBC, CTR, ECB modes
Asymmetric Encryption	RSA (up to 4096 bit key), ECC (up to 256 bit key)
Cryptographic Signature	RSA, ECDSA
Cryptographic Hash	SHA1, SHA2, SHA256
Message Authentication Code	HMAC, CMAC
Encrypted Communication	TLS, DTLS
Charging Standards	DIN SPEC 70121 – Europe ISO15118 (wired / wireless incl. Plug n' Charge) – Europe and North America GB/T 20234 – China CHAdeMO – Japan
Updates	Secure OTA
Standards Compliance	Upcoming ISO 21434 certifiable ISO 15408 certifiable up to EAL5 ISO 26262 certifiable up to ASIL D
Third-Party Support & Integration (Optional)	DXC Technolgy (security Operation Center & fleet managment) Palo Alto Networks GlobalProtect Cloud Service (end-to-end cloud security) Custom integration (upon request)

PATENTED COMMUNICATION LOCKDOWN™ METWHODOLOGY

GuardKnox's patented three-layer Communication Lockdown™ architecture enforces an ongoing, formally verified, and deterministic configuration of communication among the multiple bus networks embedded in the vehicle. The methodology enables a multi-platform and multi-service approach with the ability to host multiple operating systems and services on one chip with secure separation and full permission control.

The three layers of the Communication Lockdown™ methodology are:

Routing Layer
Verifies that the message has arrived from a legal source

Content Layer
Verifies that the content of the message, down to the bit level, is legal

Contextual Layer
Verifies the message is legitimate in the specifically functional state of the vehicle (state machine)

PATENTED SERVICES-ORIENTED ARCHITECTURE (SOA)

SOA has a secure separation (both hardware and software) between all resources, application groups, and operating systems, simplifying edge computing capabilities by providing ample processing resources with maximal flexibility both in interface support and provision for future software extensions/additional service being added. SOA patented technology creates the secure environment which enables added services and applications by hosting downloads or upgrades on The Platform throughout the lifecycle of the vehicle. The mixed criticality environment enables mission critical and non-mission critical applications to run simultaneously without interference; if one application should be compromised, all others will not be affected.

This in essence converts the driver of a vehicle to a subscriber of features and functions of the connected and/or autonomous vehicle.